

AO 106 (Rev. 04/10) Application for a Search Warrant (requesting AUSAM. Crawley) 

UNITED STATES DISTRICT COURT

for the
Eastern District of PennsylvaniaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
EMAIL ADDRESS
Stevenhoward76@yahoo.com

Case No. 19- 831-M

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See ATTACHMENT A

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. § 1028(a)

18 U.S.C. § 1341

18 U.S.C. § 1343

identity fraud

mail fraud

wire fraud


Offense Description

The application is based on these facts:

See AFFIDAVIT

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

SAMUEL A. BRACKEN, U.S. Postal Inspector

Printed name and title

Sworn to before me and signed in my presence.

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, SAMUEL A. BRACKEN, ("Affiant"), U.S. Postal Inspector, United States Postal Inspection Service, being duly sworn, depose and state as follows:

1. I am a United States Postal Inspector assigned to the Philadelphia Division of the U.S. Postal Inspection Service ("Inspection Service"), and have been so employed since February 2004. I am currently assigned to the Miscellaneous Crimes Team, which investigates violations of federal law, including identity fraud, theft of mail, aggravated identity theft, mail fraud and wire fraud, in violation of Title 18, United States Code, Sections 1028(a), 1708, 1028A, 1341 and 1343, respectively. I have received training in investigating identity theft, credit card fraud, wire fraud, counterfeit check fraud, and mail fraud offenses, including attending seminars and conferences hosted by the Inspection Service, the United States Department of Justice, the International Association of Financial Crimes Investigators, and various other law enforcement entities. During my employment as an Inspector, I have participated in hundreds of investigations involving identity fraud, theft of mail, aggravated identity theft, mail fraud, and wire fraud. In addition, I have been the Inspection Service's case agent on numerous investigations involving these offenses.

PURPOSE OF AFFIDAVIT

2. I submit this affidavit pursuant to Title 18, United States Code, Section 2703, in support of an application for a warrant to search the electronic communications contained in the following email account controlled by Oath Holdings Inc.:

"CHRIS WRIGHT" EMAIL ADDRESS
Stevenhoward76@yahoo.com

I also request certain subscriber and log records associated with this email account, as described in Attachment A, which is attached to this affidavit and incorporated by reference. The email

account that is the subject of this search warrant application is controlled by Oath Holdings Inc., 701 First Avenue, Sunnyvale, CA 94089. This application seeks a warrant to search the aforementioned email account (“the subject account”) for evidence, fruits and instrumentalities of violations of 18 U.S.C. § 1028(a) – identity fraud; 18 U.S.C. § 1341 – mail fraud; 18 U.S.C. § 1343 – wire fraud; and 18 U.S.C. § 371 – conspiracy to commit offenses against the United States (i.e., identity fraud, mail fraud and wire fraud); and to seize such evidence, fruits and instrumentalities of these crimes.

3. Unless otherwise stated, the information contained in this affidavit is personally known to me or has been related to me by others, including other law enforcement agents and officers, and/or obtained via review of various documents and records as more particularly described below. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts I believe are necessary to establish probable cause to believe that fruits, instrumentalities and evidence of violations of federal law will be found within the email account that is the subject of this affidavit.

INTRODUCTION

4. As stated in detail below, since approximately June of 2016, thousands of counterfeit payroll checks with a face value of more than \$1,000,000 have been cashed or attempted to be cashed by a group of men who have travelled to more than 35 different states and dozens of different Walmart stores within those states. These individuals have acquired personal identifying information (“PII”) of numerous innocent persons, including their names, dates of birth, social security numbers, and have used this PII to obtain fraudulent identification cards, which they presented at the Walmart stores in order to cash the counterfeit payroll checks.

Investigation has shown that an individual using the name “Chris Wright” and the email address “**stevenhoward76@yahoo.com**” produced some if not all of the fraudulent identification cards that the schemers presented at the Walmart stores in order to cash the counterfeit payroll checks. Having identified at least some of the schemers, nine of whom stand charged in an indictment in this district, and six of whom have pleaded guilty to the charges, your affiant now seeks a warrant to search the email address “**stevenhoward76@yahoo.com**” (the “subject email address”).

THE INVESTIGATION

5. On December 11, 2018, a grand jury in the Eastern District of Pennsylvania returned an 18-count superseding indictment against the following nine defendants: Ahmad BECOATE, Jeffrey ROACH, Jethro RICHARDSON, Nathaniel JONES, Jared MILLER, JuQuan HARVEY, Robert HARRINGTON, Leander ROWELL, and Brian CHERRY. The indictment charges that beginning no later than June 2016 and continuing until at least July 2018, these defendants and others conspired and schemed to present thousands of counterfeit payroll checks, with a total face value of over \$1,000,000, at Walmart stores located across the United States, in violation of Title 18, United States Code, Sections 371, 1343, 513 and 1028A, and Title 42, United States Code, Section 408(a)(7)(B). The case was assigned to the Honorable Joseph F. Leeson, Jr., under Criminal No. 18-291. The case remains pending; six defendants have pleaded guilty and three await trial.

6. Along with agents of the United States Secret Service and the Social Security Administration - Office of Inspector General, the Inspection Service conducted an investigation that led to the initial indictment and the December 2018 superseding indictment. I am the Inspection Service's case agent in that investigation. During the investigation, your affiant

learned from Walmart representatives that at some Walmart store locations, Walmart permitted customers to cash payroll checks. When a customer presented a payroll check to a Walmart employee for cashing, the customer was required to enter his or her social security number ("SSN") into a keypad and provide proper identification, usually a state driver's license or identification card. The Walmart employee scanned the check through a check reader. Certain information, including the account number of the bank account on which the payroll check was drawn; the drawee bank's routing number; and the SSN provided by the customer, was transmitted via interstate wire transmission from the Walmart store's computer system to the computer servers of a contractor for Walmart. The contractor's computer servers were located in Chicago, Illinois and St. Petersburg, Florida. The contractor analyzed the data provided by the check and the Walmart customer, then transmitted an interstate wire communication from its computer servers back to the Walmart store, recommending that Walmart accept, or decline, to cash the payroll check.

7. As part of the investigation, my co-case agents and I interviewed a co-conspirator who participated in the counterfeit check scheme, who was charged in the indictment, pleaded guilty pursuant to a cooperation plea agreement, and presently awaits sentencing ("Cooperating Defendant 1" or "CD 1"). CD 1 explained that he and others obtained, from what CD 1 termed a "Russian website," the personal identifying information ("PII") of innocent persons to use as payees on counterfeit checks that members of the group manufactured. CD 1 also stated that he and other members of the group used their cellular telephones to communicate with each other; to store PII, including social security numbers ("SSNs"), for use when cashing counterfeit checks at the Walmart stores; and to send each other fraudulent drivers' license information to use in

cashing the counterfeit checks. According to CD 1, members of the group transmitted this information to each other via text messages and emails.

8. Also as part of the investigation, my co-case agents and I obtained and executed warrants to search eight email accounts. These email accounts belonged to Ahmad BECOATE, Jeffrey ROACH, Jared MILLER, JuQuan HARVEY, Leander ROWELL, and Jethro RICHARDSON, and were being used by six of the group members, all of whom were eventually indicted in Criminal No. 18-291. Analysis of the material obtained through the searches of the eight email accounts showed that these accounts contained PII, including PII that had been used in passing counterfeit checks at Walmart locations. Analysis also showed that five of the eight accounts had communicated with the email address "**stevenhoward76@yahoo.com**" in order to obtain fraudulent identification cards to further the scheme of cashing counterfeit checks. These emails to "**stevenhoward76@yahoo.com**" show the defendants requesting counterfeit identification cards of various states, providing information relating to payment for the counterfeit identification cards, and requesting that the identification cards be sent via Federal Express to various locations in the United States, including in the Eastern District of Pennsylvania.

**ANALYSIS OF EMAIL COMMUNICATIONS TO
"STEVENHOWARD76@YAHOO.COM" and "CRAZYSWAGG87@GMAIL.COM"**

9. Analysis of email account "**crazyswagg87@gmail.com**," one of the accounts searched pursuant to the search warrant, revealed approximately 183 emails to and from "**stevenhoward76@yahoo.com**." These emails were sent and received from November 2017 through February 2018. Investigation revealed that the email account "**crazyswagg87@gmail.com**" belonged to defendant Ahmad BECOATE.

10. A review of these emails revealed conversations in which BECOATE is requesting counterfeit identification cards from **“stevenhoward76@yahoo.com.”** The emails also show BECOATE providing **“stevenhoward76@yahoo.com”** with proof that payment was sent for the purchase of the counterfeit identification cards via Western Union. BECOATE would then send **“stevenhoward76@yahoo.com”** directions on where to ship the counterfeit identification cards, depending on BECOATE’s current location at the time of the email.

11. For example, between November 17, 2017 and November 21, 2017, the following email conversation was had between **“crazyswagg87@gmail.com”** and **“stevenhoward76@yahoo.com”**:

- **“Crazyswagg87@gmail.com”** sent the following - “Yooo did you send them jawns to west v” (It should be noted that **“stevenhoward76@yahoo.com”** is titled and saved as “Dred Head” by BECOATE)
- **“stevenhoward76@yahoo.com”** replied – “Naw I didn’t get address to send them.” and asked “Which ones are you talking about.”
- **“crazyswagg87@gmail.com”** replied – “Can you send out tonight?? I’ll send the \$100 I owe in 30 mins ok”
- **“stevenhoward76@yahoo.com”** replied – “Can you resend the info cause I don’t have the email.”
- **“crazyswagg87@gmail.com”** replied – “The western Union info??? This for the NJ and WA jawns”
- **“stevenhoward76@yahoo.com”** replied – “Ohh okay I been texting you all day for shipping address.”

- “crazyswagg87@gmail.com” replied – “That’s my right hand you been texting, he in a coma...hold on I’m finna send you the shipping info”
- “stevenhoward76@yahoo.com” replied – “Let me know when you send everything.”
- “crazyswagg87@gmail.com” replied with an image capture of information for a FedEx Office Center located at 4215 W Wendover Avenue, Unit F, Greensboro, NC 27407 and the following text “And I’m finna send the money, the other \$100 in 20 minutes” and then an image of a Western Union receipt with a payment to “Chris Wright” of Money Transfer Control Number “MTCN” 3971 35 3202 from Ahmad BECOATE.
- “crazyswagg87@gmail.com” asks the following – “Did you send it out??” and then asks “I never told you where to send it?”
- “stevenhoward76@yahoo.com” replied – “Naw you never sent me address to send it to.”
- “crazyswagg87@gmail.com” replied with an image capture of information for a FedEx Office Center located at 218 Griffin Road, Portsmouth, NH 03801 and then in another email states “Let me know when you send it out” and then in another email states “Don’t forget to send off you” and in another email states “Yo this the nigga that need the Jersey and Washington... send it to the New Hampshire Fedex office.”
- “stevenhoward76@yahoo.com” replied – “Cool it’s already sent.”
- “crazyswagg87@gmail.com” replied – “Yo why did you send it in that name you have my name man... AHMAD BECOATE!!! HOW AM I

SUPPOSED TO GET THE PACKAGE????? YOU BEEN SENDING ME THIS SHIT FOR A MINUTE YO... I NEED YOU TO CALL AND CHANGE THE NAME OR ADD MINES”

- “**stevenhoward76@yahoo.com**” replied – “I’m out of town and I had one of my assistance send it. I just texted you and you said you picked it up already.” and then in another email states “I apologize for the inconvenience. I had one of my associates send it so they didn’t know what name to put on there so they just made one up. Next time I make sure to put Ahmad. Sorry for the inconvenience again.”
- “**crazyswagg87@gmail.com**” replied – “It’s resolved yo. Thanks! But did you get the \$100 I sent cause I need an AZ id now? I’m sending the other \$70 now...”

12. Records obtained from Western Union revealed the following payments from BECOATE to an individual named Chris Wright:

- November 16, 2017 - \$320.00 sent via Western Union MCTN #3514552599 from BECOATE to Wright. The money was picked up by Wright at the Kroger Grocery Store located at 4550 Jonesboro Road, Union City, GA. Western Union records show that the individual using the name Chris Wright provided Western Union with Pennsylvania driver’s license #51491629 in order to retrieve the money. I conducted a query in NCIC for Pennsylvania driver’s license #51491629 in NCIC and discovered that this license number does not exist.

- November 17, 2017 - \$100.00 sent via Western Union MCTN #3971353202 from BECOATE to Wright. The money was picked up by Wright at a Kroger Grocery Store located at 4550 Jonesboro Road, Union City, GA. Western Union records show that the individual using the name Chris Wright provided Western Union with Pennsylvania driver's license #51491629 in order to retrieve the money. As mentioned above, this Pennsylvania driver's license number, #51491629, does not exist.

13. Records obtained from Fedex show the following shipment related to BECOATE's order of counterfeit identification cards:

- November 20, 2017 – Fedex shipment #788540377059 from J. Anthony, 7058 Bayrose Circle, Atlanta, GA to Eric Brown, 218 Griffin Road, Portsmouth, NH. BECOATE had requested a shipment to this location, a Fedex store, and per his email, he was upset because the package was not sent in his, BECOATE's, name.

14. The email records of this BECOATE email account show that on November 22, 2017, further email communication was had between "crazyswagg87@gmail.com" and "stevenhoward76@yahoo.com":

- "stevenhoward76@yahoo.com" sent the following emails – "Let me know when you send the rest funds and shipping address for Arizona." and "Glad it got resolved."
- "crazyswagg87@gmail.com" replied with a message in the subject line "This the Mtcn for the \$70 everything else is still the same" along with an image of MTCN 4782420514 sent to Chris Wright via Western Union from Ahmad

BECOATE. Another message was sent with a message in the subject line "Yooo all the info is the same just give them this Mtcn. I sent it on the western union app." A third message was sent replying "Did you get the Mtcn info???"

- "stevenhoward76@yahoo.com" replied – "Yeah I got the mtcn. Where do I ship it."
- "crazyswagg87@gmail.com" replied with an image capture of information for a FedEx Office Store located at 3535 Market Street, Philadelphia, PA.

15. Records obtained from Western Union revealed the following payments from BECOATE to an individual named Chris Wright:

- November 22, 2017 - \$70.00 sent via Western Union MCTN #4782420514 from BECOATE to Wright. The money was picked up by Wright at a Kroger Grocery Store located at 4550 Jonesboro Road, Union City, GA. Western Union records show that the individual using the name Chris Wright provided Western Union with Pennsylvania driver's license #51491629 in order to retrieve the money. As mentioned above, I conducted a query in NCIC for this Pennsylvania driver's license number, #51491629, and discovered it did not exist.

16. The email records of this BECOATE email account show that further email communication was had between "crazyswagg87@gmail.com" and "stevenhoward76@yahoo.com" between January 6, 2018 to January 10, 2018:

- "crazyswagg87@gmail.com" sent the following – "Yo I need a New Jersey – make it scannable with this info:

Ahmad Jamaal Becoate

01/13/1987

5'10

197lbs

Black hair

Brown Eyes

ID number B2736 34771 01872

2881 Mt Ephraim Ave, Camden, NJ 08104

How much?"

- **"stevenhoward76@yahoo.com"** replied – "200" and with another message stated "200 including the shipping fee. So just 30 dollars more. Let me know if you want me to get started on that."
- **"crazyswagg87@gmail.com"** replied – "Ok. I'll let you know." And with another message stating "Yoo you can go ahead and start on that jawn. I'll send the money about 5."
- **"stevenhoward76@yahoo.com"** replied – "Okay cool" and with another message stated "Just wondering if you wanted the face sent today. Just send shipping address and I still haven't received the funds info."
- **"crazyswagg87@gmail.com"** replied – "I'm gone send in the next 30 mins" and with an image capture of information for a FedEx Office Store located at 3232 Crain Hwy Suite A, Waldorf, MD. Further messages were sent stating "Waiting for my homie to send the bread." And "Ahmad Becoate Sent from Virginia Western Union \$220 Mtcn-837-336-9246" and "yo lemme know when you get it".

- “**stevenhoward76@yahoo.com**” replied – “What’s good bro just saw your email. It will be shipped tomm. I’m shipping it to the Maryland fedex shipping center.”
- “**crazyswagg87@gmail.com**” replied – “Yo what’s good! Send it to this address:” along with an image capture of information for a FedEx Office Store located at 4215 W Wendover Ave F, Greensboro, NC 27407.

17. Records obtained from Western Union revealed the following payments from BECOATE to an individual named Chris Wright:

- January 9, 2018 - \$220.00 sent via Western Union MCTN #8373369246 from BECOATE to Wright. The money was picked up by Wright at a Kroger Grocery Store located at 4550 Jonesboro Road, Union City, GA. Western Union records show that the individual using the name Chris Wright provided Western Union with Pennsylvania driver’s license #51491629 in order to retrieve the money. As mentioned above, a query in NCIC for Pennsylvania driver’s license #51491629 shows that this license number does not exist.

18. Records obtained from Fedex show the following shipment related to BECOATE’s order of counterfeit identification cards:

- January 10, 2018 – Fedex shipment #789305178210 from J. Anthony, 7058 Bayrose Circle, Atlanta, GA to Ahmad Becoate, 4215 W Wendover Ave F, Greensboro, NC.

19. The email records of this BECOATE email account show that on February 12, 2017, further email communication was had between “**crazyswagg87@gmail.com**” and “**stevenhoward76@yahoo.com**”:

- “crazyswagg87@gmail.com” sent the following – “Yooo I need you. Send me a Virginia with nothing on it. Use my face”. Included in the email was a photograph of BECOATE. Another message was sent that added, “Can you get it out today???”
- “stevenhoward76@yahoo.com” replied – “Yeah. Just send the shipping and mtcn info.”
- “crazyswagg87@gmail.com” replied – “Ahmad Becoate Sent from Oklahoma \$170 Western union MTCN-685-103-5129” along with an image capture of information for a FedEx Office Store located at 8228 E 61st St Suite 105, Tulsa, OK. Further messages were sent stating “Let me know when you send it out. I am out of town” and “Did you send it out”.
- “stevenhoward76@yahoo.com” replied – “Not yet. Sending it in next 20 min. Why what’s up.”
- “crazyswagg87@gmail.com” replied – “Because I’m leaving tomorrow morning when it gets here.”
- “stevenhoward76@yahoo.com” replied – “It’s sent it will be there by 1030 in am.”

20. Records obtained from Western Union revealed the following payments from BECOATE to an individual named Chris Wright:

- February 12, 2018 - \$170.00 sent via Western Union MCTN #6851035129 from BECOATE to Wright. The money was picked up by Wright at the Kroger Grocery Store located at 4550 Jonesboro Road, Union City, GA. Western Union records show that the individual using the name Chris Wright provided Western

Union with Pennsylvania driver's license #51491629 in order to retrieve the money. As noted above, a query in NCIC for this Pennsylvania driver's license #51491629 shows that it does not exist.

21. Records obtained from Fedex show the following shipment related to BECOATE's order of counterfeit identification cards:

- February 12, 2018 – Fedex shipment #789711506436 from J. Anthony, 7058 Bayrose Circle, Atlanta, GA to A. Becoate, 8228 E 61st St Ste 105, Tulsa, OK.

**ANALYSIS OF EMAIL COMMUNICATIONS TO
“STEVENHOWARD76@YAHOO.COM” AND OTHER DEFENDANTS**

22. Analysis of the email account “mochaboy69@gmail.com,” another one of the accounts searched pursuant to the search warrant, revealed approximately 30 messages exchanged between “**stevenhoward76@yahoo.com**”. These emails were exchanged in February/March 2017 and February 2018. Investigation revealed the email account “mochaboy69@gmail.com” belonged to defendant Leander ROWELL. Some examples of the messages exchanged with “**stevenhoward76@yahoo.com**” include the following:

- February 21, 2017 – “mochaboy69@gmail.com” sent the following – “Yooooooooo I need your number”
- February 21, 2017 – “**stevenhoward76@yahoo.com**” replied – “Ight I got u. I’m hit u tomm”
- February 21, 2017 – “mochaboy69@gmail.com” replied – “Cool”
- February 22, 2017 – “**stevenhoward76@yahoo.com**” replied – “Bro u can hit me on the same line I just added mins to it. Let me know what u need”

- February 22, 2017 – “mochaboy69@gmail.com” replied – “A COMPLETELY BLANK ARKANSAS”
- February 22, 2017 – “**stevenhoward76@yahoo.com**” replied – “Ight cool let me where to send”
- February 28, 2017 – “mochaboy69@gmail.com” replied – “Ok ima hit u tonight”
- February 28, 2017 – “mochaboy69@gmail.com” wrote – “I want a, completely blank Arkansas No sig No nothing”

23. Analysis of the email account, “jlmiller1286@gmail.com,” another one of the accounts searched pursuant to the search warrant, revealed approximately seven messages exchanged between “**stevenhoward76@yahoo.com**.” These emails were exchanged between January 2017 and March 2017. Investigation revealed the email account “jlmiller1286@gmail.com” belonged to defendant Jared MILLER. Some examples of the messages exchanged with “**stevenhoward76@yahoo.com**” include the following:

- January 9, 2017 – “jlmiller1286@gmail.com” sent the following – “hey u still in biz?”
- January 9, 2017 – “jlmiller1286@gmail.com” sent the following – “Kentucky blank except signature and governors info” along with a photograph of himself (Jared MILLER)
- February 28, 2017 – “jlmiller1286@gmail.com” sent the following – two photographs, one of an unknown black male and another of a MoneyGram receipt for \$170.00 showing MoneyGram transfer #890542314 sent on February 27, 2017

to "Chris Wright". Text included in the message was "Kristopher Nichols.

8/20/1978 3006 weaver ct Augusta ga 30906 6-1 212lbs"

- February 28, 2017 – "stevenhoward76@yahoo.com" replied – "What is the sender name and where do I send it."
- February 28, 2017 – "stevenhoward76@yahoo.com" further replied – "Let me know so I can send it to you. Need the sender name and shipping address"

24. Analysis of the email account, "j_black009@yahoo.com", one of the accounts searched pursuant to the search warrant, revealed one email message sent to "stevenhoward76@yahoo.com" on July 26, 2016. Investigation revealed the email account "j_black009@yahoo.com" belonged to defendant Jeffrey ROACH. This message included the following:

- July 26, 2016 – "j_black009@yahoo.com" sent the following –
"WISCONSIN ID-----NO ID NUMBER
NO ID NUMBER
NO NAME
NO ADDRESS
NO DATE OF BIRTH
NO ISSUE DATE
NO EXPIRATION DATE
NO SIGNATURE
Sex: male
Height: 6'2

Weight: 220

Eyes: brown”

Included in the message was a photograph of Robert HARRINGTON.

IDENTIFYING THE FALSE ID MAKER

25. The nine indicted co-defendants have all been arrested in connection with either the initial indictment or the December 11, 2018 superseding indictment. Several of the defendants agreed to speak with the government regarding their involvement in the scheme to cash counterfeit checks. One of the cooperating defendants mentioned above (CD 1) provided the following information on the individual who provided the counterfeit identification cards needed to cash the counterfeit checks.

- CD 1 stated that the fraudulent identification cards used by himself and others came from an individual in the Atlanta, GA area named “Andy.” CD 1 advised that he paid “Andy” approximately \$150 to \$175 for a fraudulent identification card, and would pay “Andy” by sending money via Western Union. CD 1 stated he would send the money via Western Union to “Cory or Chris Wright,” though CD 1 stated that he didn’t believe this to be “Andy’s” real name. CD 1 stated that he would order a fraudulent identification card from “Andy” by sending “Andy” an email requesting a “face.” CD 1 advised agents that the email address through which he communicated with “Andy” was “stevenhoward,” or something close to that, at yahoo.com. CD 1 estimated that at least five of the co-defendants in this case would get their fraudulent identification cards from “Andy.” CD 1 added further details during a second interview reiterating CD 1’s previous statement and also providing information on meeting “Andy” on one

occasion in 2011 or 2012 at the Varsity Hamburger restaurant in Atlanta, GA.

CD 1 said he met "Andy" and described him as a light skinned black male, approximately 5'10" tall, slender build, with dread locks.

26. A second cooperating defendant (CD 2) provided the following information on the individual who provided the counterfeit identification cards needed to cash the counterfeit checks:

- CD 2 stated the fraudulent identification cards came from an individual named "Chris Wright" in Atlanta, GA. CD 2 advised that he communicated with "Wright" via an email address, "stevenhoward@yahoo.com", and that he would request a fraudulent identification card with an email requesting a "face." CD 2 stated that he also communicated with "Wright" via text messaging on his cellular telephone. CD 2 stated that "Wright" was saved in his phone as "BMAN." CD 2 stated that the cost of the fraudulent identification cards was approximately \$150 per card, plus a \$25 overnight shipping charge. CD 2 advised he paid "Wright" via MoneyGram sent to the Atlanta, GA area.

REVIEW OF CELLULAR TELEPHONE OF CD 2

27. During the course of the investigation, CD 2's cellular telephone was taken into custody as evidence. A search warrant was obtained for CD 2's cellular telephone and a review found text message communications with an individual saved as "BMAN" with a telephone number of 404-426-6144. 404 is an area code located in the Atlanta, GA area. Subscriber records were obtained for cellular telephone number 404-426-6144 and it was found registered to the following individual since August 5, 2013:

- **Subscriber Name:** Steven Howard

- **Subscriber Email: Stevenhoward76@yahoo.com**

The records obtained showed that cellular telephone number 404-426-6144 was still active as of March 2019. The records showed that this telephone number belonged to a prepaid account.

28. There were approximately 131 text messages between CD 2 and "BMAN" between November 2017 and July 2018. The following are excerpts of the texts between the two which appear to relate to orders of fraudulent identification cards:

- November 20, 2017 - CD 2 to BMAN: "Hey he said he sent the mailing address to your email"
- November 20, 2017 - BMAN to CD 2: "Yeah I sent it to new ham address"
- November 21, 2017 - CD 2 to BMAN: "Cool thank you"
- November 21, 2017 - BMAN to CD 2: "Track number 788540377059 receiver name eric brown"
- November 21, 2017 - CD 2 to BMAN: "Good morning is the fedex tracking number"
- November 21, 2017 - BMAN to CD 2: "Yeah"
- November 21, 2017 - CD 2 to BMAN: "He has it"
- November 21, 2017 - CD 2 to BMAN: "Thanks bro"

29. This conversation appears to relate to the email conversation between BECOATE with his "crazyswagg87@gmail.com" and "stevenhoward76@yahoo.com," during the approximate same time period from November 17, 2017 to November 21, 2017. The email conversation appears to show BECOATE ordering fraudulent identification cards, sending

payment via Western Union, and the fraudulent identification cards being shipped from the Atlanta, GA area to a FedEx store located in Portsmouth, NH.

30. Further review of the text messaging between CD 2 and "BMAN" revealed the following:

- December 12, 2017 – CD 2 to BMAN: "Morning bro check ya email my boy said he sent you a message"
- December 12, 2017 – CD 2 to BMAN: "Ahmad Becoate Sent from Indiana \$170 Western union Mtcn-747-330-7545"
- December 12, 2017 – BMAN to CD 2: "Cool"
- December 12, 2017 – BMAN to CD 2: "Did the guy from last week still want his."
- December 12, 2017 – CD 2 to BMAN: "Oh crap my fault I forgot I'm on way to dude crib now I'll find out"
- December 12, 2017 – CD 2 to BMAN: "Bro can you send that out tonight"
- December 12, 2017 – CD 2 to BMAN: "And the other dude said he will get it next week something came up"

31. A review of records for Western Union revealed that on December 12, 2017, Ahmad BECOATE sent \$170 via Western Union MTCN #747-330-7545 to Chris Wright. The money was picked up by Wright at a Kroger Grocery Store located at 6055 Old National Highway, College Park, GA. Western Union records show that the individual using the name Chris Wright provided Western Union with Pennsylvania driver's license #51491629 in order to

retrieve the money. As noted above, a query for Pennsylvania driver's license #51491629 in NCIC showed that that driver's license number was non-existent.

32. Further review of the text messaging between CD 2 and "BMAN" revealed the following:

- June 7, 2018 – BMAN to CD 2: "Bro where do I ship and funds info so I can ship it."
- June 8, 2018 – CD 2 to BMAN: "My bad bro I was sick as shit yesterday"
- June 8, 2018 – CD 2 to BMAN: "Will send money today cause I need it by tomorrow"
- June 8, 2018 – CD 2 to BMAN: "Broooooo!!!!!"
- June 8, 2018 – CD 2 to BMAN: "Money gram Reference number 757-525-41 \$325 Check email"
- June 8, 2018 – CD 2 to BMAN: "Broooooo"
- June 9, 2018 – BMAN to CD 2: "You sent another one"
- June 9, 2018 – CD 2 to BMAN: "Yeah"
- June 11, 2018 – CD 2 to BMAN: "Bro don't forget to send those out to me today"
- June 11, 2018 – CD 2 to BMAN: "Need them"
- June 11, 2018 – BMAN to CD 2: "Need address"
- June 11, 2018 – CD 2 to BMAN: "Jeffrey Roach 516 S Macon St Baltimore MD 21224"

33. A review of FedEx records revealed a shipment sent to Jeffrey Roach on June 11, 2018 from J Anthony shipped from Hapeville, GA.

FEDEX RECORDS

34. As described in previous paragraphs, records were obtained from FedEx for shipments to the defendants, or the defendants' addresses. A review of FedEx records revealed 18 packages that were identified as being possibly involved in the scheme. They all exhibited similar characteristics, being shipped to a defendant or a defendant's address, shipped from the same name (a variation of Jay Anthony), shipped mainly from the Atlanta, GA area, and all having a similar weight. Please note that the return address is what was listed on the shipping label and does not correspond to the actual location where the item was shipped from. In each instance, a FedEx account number was used to ship the packages belonging to two companies believed to be without the companies' knowledge or consent.

Ship Date	Sent To	Sent To Address	Shipped From, As Listed	Return Address Listed	Shipped From Location	Tracking Number	Weight
4/7/2017	Jeffrey Roach	8406 Hamlin Street, Lanham, MD	Jay Anthony	7058 Bayrose Circle, Atlanta, GA	Marietta, GA	786174339795	.5 pounds
5/22/2017	Jeffrey Roach	8406 Hamlin Street, Lanham, MD	J Anthony	7058 Bayrose Circle, Atlanta, GA	Hapeville, GA	786654401395	.5 pounds
7/6/2017	Julius Lee	8406 Hamlin Street, Lanham, MD	Jay Anthony	41 Rachel Drive, Nashville, TN	Bartlett, TN	787105328772	.5 pounds
8/28/2017	Jeffrey Roach	8406 Hamlin Street, Lanham, MD	J. Anthony	7058 Bayrose Circle, Atlanta, GA	Fayetteville, GA	787537390914	.5 pounds
9/21/2017	Juquan Harvey	8406 Hamlin Street, Lanham, MD	J. Anthony	7068 Bayrose Circle, Atlanta, GA	Hapeville, GA	787814593905	.5 pounds

Ship Date	Sent To	Sent To Address	Shipped From, As Listed	Return Address Listed	Shipped From Location	Tracking Number	Weight
10/19/2017	Jeffrey Roach	8406 Hamlin Street, Lanham, MD	J. Anthony	7058 Bayrose Circle, Atlanta, GA	Hapeville, GA	788145535118	.5 pounds
11/2/2017	Jeffrey Roach	8406 Hamlin Street, Lanham, MD	J Anthony	1 Duette Way, Broomfield, CO	Fayetteville, GA	788312511662	.5 pounds
11/2/2017	Ahmad Becoate	4215 W. Wendover Ave F, Greensboro, NC	J Anthony	1 Duette Way, Broomfield, CO	Fayetteville, GA	788312555168	.5 pounds
11/20/2017	Eric Brown	218 Griffin Road, Portsmouth, NH	J. Anthony	7058 Bayrose Circle, Atlanta, GA	Hapeville, GA	788540377059	.5 pounds
1/2/2018	Ahmad Becoate	3208 W Gate City Blvd, Greensboro, NC	J. Anthony	7058 Bayrose Circle, Atlanta, GA	Hapeville, GA	789195941365	.5 pounds
1/10/2018	Ahmad Becoate	4215 W. Wendover Ave F, Greensboro, NC	J. Anthony	7058 Bayrose Circle, Atlanta, GA	Hapeville, GA	789305178210	.5 pounds
2/12/2018	A.Becoate	8228 E 61 st St, Ste 105, Tulsa, OK	J. Anthony	7058 Bayrose Circle, Atlanta, GA	Hapeville, GA	789711506436	.5 pounds
5/18/2018	Leander Rowell	449 Tate Street, Suite A, Greensboro, NC	J Anthony	1 Duette Way, Broomfield, CO	Fayetteville, GA	781034477297	.5 pounds
5/22/2018	T Jones	506 Ashburn Street, High Point, NC	J Anthony	1 Duette Way, Broomfield, CO	Hapeville, GA	781086987895	.5 pounds
6/11/2018	Jeffrey Roach	516 S Macon Street, Baltimore, MD	J Anthony	1 Duette Way, Broomfield, CO	Hapeville, GA	781374477325	.5 pounds

Ship Date	Sent To	Sent To Address	Shipped From, As Listed	Return Address Listed	Shipped From Location	Tracking Number	Weight
8/3/2018	Leander Rowell	812 Bilbro Street, Greensboro, NC	J Anthony	1 Duette Way, Broomfield, CO	Hapeville, GA	782139760268	.5 pounds
9/18/2018	Leander Rowell	812 Bilbro Street, Greensboro, NC	J. Anthony	1 Duette Way, Broomfield, CO	Hapeville, GA	782832715465	.5 pounds
2/4/2019	Lee Rowell	812 Bilbro Street, Greensboro, NC	J Anthony	1 Duette Way, Broomfield, CO	Hapeville, GA	785314217611	.5 pounds

WESTERN UNION AND MONEYGRAM

35. As described in the previous paragraphs, records were obtained from Western Union and MoneyGram for payments from the defendants to “Chris Wright.” A review of the records obtained from Western Union and MoneyGram revealed approximately 76 payments to “Chris Wright” totaling \$15,997.00:

Date	Amount	Sender Name	Recipient Name	Recipient Location	Company
8/10/2013	\$470.00	Jared MILLER	Chris Wright	College Park, GA	Western Union
8/16/2013	\$320.00	Jeffrey ROACH	Chris Wright	College Park, GA	Western Union
8/22/2013	\$420.00	Jeffrey ROACH	Chris Wright	College Park, GA	MoneyGram
8/24/2013	\$170.00	Jeffrey ROACH	Chris Wright	Riverdale, GA	MoneyGram
9/9/2013	\$150.00	Jeffrey ROACH	Chris Wright	College Park, GA	MoneyGram
9/9/2013	\$20.00	Jeffrey ROACH	Chris Wright	College Park, GA	MoneyGram
10/7/2013	\$320.00	Jeffrey ROACH	Chris Wright	College Park, GA	MoneyGram
10/24/2013	\$220.00	Jeffrey ROACH	Chris Wright	College Park, GA	MoneyGram
12/4/2013	\$470.00	Jeffrey ROACH	Chris Wright	College Park, GA	MoneyGram

Date	Amount	Sender Name	Recipient Name	Recipient Location	Company
1/12/2014	\$320.00	Jared MILLER	Chris Wright	College Park, GA	Western Union
4/7/2014	\$170.00	Jeffrey ROACH	Chris Wright	"Internal Correction"	MoneyGram
4/8/2014	\$172.00	Jeffrey ROACH	Chris Wright	Riverdale, GA	MoneyGram
5/1/2014	\$320.00	Jared MILLER	Chris Wright	College Park, GA	Western Union
7/28/2014	\$150.00	Ahmad BECOATE	Chris Wright	College Park, GA	MoneyGram
8/5/2014	\$170.00	Ahmad BECOATE	Chris Wright	College Park, GA	Western Union
8/11/2014	\$170.00	Ahmad BECOATE	Chris Wright	College Park, GA	Western Union
9/3/2014	\$320.00	Jeffrey ROACH	Chris Wright	College Park, GA	MoneyGram
10/13/2014	\$170.00	Jeffrey ROACH	Chris Wright	College Park, GA	MoneyGram
11/20/2014	\$175.00	Jared MILLER	Chris Wright	Union City, GA	Western Union
12/15/2014	\$170.00	Ahmad BECOATE	Chris Wright	Riverdale, GA	MoneyGram
3/2/2015	\$170.00	Ahmad BECOATE	Chris Wright	Riverdale, GA	MoneyGram
3/18/2015	\$290.00	Jared MILLER	Chris Wright	East Point, GA	MoneyGram
3/30/2015	\$320.00	Ahmad BECOATE	Chris Wright	Riverdale, GA	MoneyGram
4/13/2015	\$320.00	Ahmad BECOATE	Chris Wright	East Point, GA	MoneyGram
4/16/2015	\$170.00	Ahmad BECOATE	Chris Wright	East Point, GA	MoneyGram
5/19/2015	\$170.00	Ahmad BECOATE	Chris Wright	Riverdale, GA	MoneyGram
6/9/2015	\$175.00	Ahmad BECOATE	Chris Wright	East Point, GA	MoneyGram
8/3/2015	\$170.00	Jeffrey ROACH	Chris Wright	Riverdale, GA	MoneyGram
8/10/2015	\$170.00	Ahmad BECOATE	Chris Wright	Union City, GA	MoneyGram
9/14/2015	\$320.00	Ahmad BECOATE	Chris Wright	College Park, GA	MoneyGram
9/30/2015	\$170.00	JuQuan HARVEY	Chris Wright	Union City, GA	MoneyGram

Date	Amount	Sender Name	Recipient Name	Recipient Location	Company
10/5/2015	\$320.00	Jeffrey ROACH	Chris Wright	Riverdale, GA	MoneyGram
10/8/2015	\$170.00	Jeffrey ROACH	Chris Wright	College Park, GA	MoneyGram
12/8/2015	\$120.00	Jeffrey ROACH	Chris Wright	Union City, GA	MoneyGram
12/8/2015	\$220.00	JuQuan HARVEY	Chris Wright	Union City, GA	MoneyGram
12/23/2015	\$300.00	Ahmad BECOATE	Chris Wright	Union City, GA	MoneyGram
12/30/2015	\$170.00	Ahmad BECOATE	Chris Wright	Union City, GA	MoneyGram
1/21/2016	\$320.00	Ahmad BECOATE	Chris Wright	"Internal Correction"	MoneyGram
1/27/2016	\$20.00	Ahmad BECOATE	Chris Wright	Riverdale, GA	MoneyGram
2/2/2016	\$170.00	Ahmad BECOATE	Chris Wright	Riverdale, GA	MoneyGram
3/2/2016	\$170.00	Ahmad BECOATE	Chris Wright	Riverdale, GA	MoneyGram
3/3/2016	\$170.00	Jared MILLER	Chris Wright	Union City, GA	Western Union
4/11/2016	\$170.00	Ahmad BECOATE	Chris Wright	College Park, GA	MoneyGram
4/27/2016	\$170.00	Ahmad BECOATE	Chris Wright	Union City, GA	MoneyGram
6/14/2016	\$170.00	Jeffrey ROACH	Chris Wright	Riverdale, GA	MoneyGram
7/11/2016	\$170.00	Jeffrey ROACH	Chris Wright	Riverdale, GA	MoneyGram
7/18/2016	\$150.00	Jeffrey ROACH	Chris Wright	East Point, GA	MoneyGram
7/18/2016	\$20.00	Jeffrey ROACH	Chris Wright	East Point, GA	MoneyGram
7/27/2016	\$170.00	Jeffrey ROACH	Chris Wright	Riverdale, GA	MoneyGram
8/26/2016	\$170.00	Jeffrey ROACH	Chris Wright	Riverdale, GA	MoneyGram
10/27/2016	\$320.00	Jeffrey ROACH	Chris Wright	Union City, GA	MoneyGram
11/2/2016	\$170.00	Ahmad BECOATE	Chris Wright	College Park, GA	Western Union
11/29/2016	\$170.00	Jeffrey ROACH	Chris Wright	Union City, GA	MoneyGram

Date	Amount	Sender Name	Recipient Name	Recipient Location	Company
3/10/2017	\$170.00	Jeffrey ROACH	Chris Wright	Riverdale, GA	MoneyGram
4/7/2017	\$170.00	Jeffrey ROACH	Chris Wright	Riverdale, GA	MoneyGram
5/19/2017	\$470.00	Jeffrey ROACH	Chris Wright	Union City, GA	MoneyGram
8/25/2017	\$170.00	Jeffrey ROACH	Chris Wright	Riverdale, GA	MoneyGram
9/21/2017	\$170.00	JuQuan HARVEY	Chris Wright	Riverdale, GA	MoneyGram
9/26/2017	\$170.00	Jeffrey ROACH	Chris Wright	Union City, GA	MoneyGram
10/18/2017	\$320.00	Jeffrey ROACH	Chris Wright	Marietta, GA	MoneyGram
11/1/2017	\$320.00	Jeffrey ROACH	Chris Wright	Marietta, GA	MoneyGram
11/6/2017	\$170.00	Ahmad BECOATE	Chris Wright	Union City, GA	Western Union
11/16/2017	\$320.00	Ahmad BECOATE	Chris Wright	Union City, GA	Western Union
11/17/2017	\$100.00	Ahmad BECOATE	Chris Wright	Union City, GA	Western Union
11/22/2017	\$70.00	Ahmad BECOATE	Chris Wright	Union City, GA	Western Union
12/12/2017	\$170.00	Ahmad BECOATE	Chris Wright	College Park, GA	Western Union
12/19/2017	\$320.00	Ahmad BECOATE	Chris Wright	Atlanta, GA	Western Union
12/29/2017	\$170.00	Ahmad BECOATE	Chris Wright	College Park, GA	Western Union
1/9/2018	\$220.00	Ahmad BECOATE	Chris Wright	College Park, GA	Western Union
1/28/2018	\$170.00	Ahmad BECOATE	Chris Wright	College Park, GA	Western Union
2/7/2018	\$170.00	Ahmad BECOATE	Chris Wright	College Park, GA	Western Union
2/12/2018	\$170.00	Ahmad BECOATE	Chris Wright	College Park, GA	Western Union
2/27/2018	\$170.00	Ahmad BECOATE	Chris Wright	College Park, GA	Western Union
5/18/2018	\$175.00	Tyrell JONES	Chris Wright	Union City, GA	Western Union
5/18/2018	\$170.00	Ahmad BECOATE	Chris Wright	College Park, GA	Western Union

Date	Amount	Sender Name	Recipient Name	Recipient Location	Company
8/2/2018	\$160.00	Leander ROWELL	Chris Wright	College Park, GA	Western Union

SUMMARY

36. Since approximately June of 2016, thousands of counterfeit payroll checks have been cashed or attempted to be cashed by a group of individuals, who have traveled to more than 35 different states and dozens of different Walmart locations within those states. These individuals have acquired the identities of numerous individuals, to include their name, date of birth, and SSN, and have used this personal identifying information to obtain fraudulent identification cards. With this information, these individuals have successfully participated in a scheme to defraud by presenting counterfeit payroll checks bearing the names of the compromised individuals, containing the routing numbers of real banks and the bank account numbers of actual businesses that were allegedly drawn on banks that did not in fact issue the checks. Based on investigation to date, these individuals have caused an intended loss of over \$1,000,000, based on the face amounts of the counterfeited checks. The investigation to date has determined that subjects Ahmad BECOATE, Jeffrey ROACH, Jethro RICHARDSON, Jared MILLER, JuQuan HARVEY, Nathaniel T. JONES, Brian CHERRY, Leander ROWELL, Robert HARRINGTON, and others known and unknown are willing participants in this scheme and have collaborated with at least one other person in the conspiracy. Through statements made by cooperating defendants, emails obtained through search warrants, and business records obtained from various companies, it appears an individual in the Atlanta, GA area was providing counterfeit identification documents to at least one participant in this scheme up through February 2019. Emails from the defendants show requests to “**stevenhoward76@yahoo.com,**”

Western Union and MoneyGram records show payment to "Chris Wright" from the defendants, and FedEx records show shipments of packages to the defendants upon payment. Two cooperating defendants have provided corroborating evidence that they ordered counterfeit identification cards came from the same source in the Atlanta GA area using an email address similar to "**stevenhoward76@yahoo.com**" and send payments to "Chris Wright".

TRAINING AND EXPERIENCE

37. Based on my training and experience, and the experience of other Inspectors and agents involved in this investigation, I know the following information regarding individuals involved in identity theft and counterfeit document production:

38. Individuals will often keep records obtained from their fraudulent document production, including requests, payments and purchases of equipment, including but not limited to emails, emailed receipts, emailed applications, etc. These documents are usually kept by the individual for future reference, for months and even years, and are often stored in the email's inbox. Such information can remain in the email account almost indefinitely.

39. Individuals who engage in identity theft and fraudulent document production frequently obtain individual victims' personal and financial information through the theft or diversion of mail, the theft of personal property, the interception of Internet transactions, compromising personal information files from a legitimate business source, or purchasing the information through the "Dark Web." This information is stored in areas for ready access and to conceal them from law enforcement. I also know that persons who commit multiple acts of identity theft and fraudulent document production typically maintain documents related to those offenses for months and even years, in order to facilitate further fraud and theft. This

information is often stored in email boxes so that it will be readily accessible from any computer or phone and so that it can be sent via email to other co-conspirators.

40. Individuals who engage in identity theft and fraudulent document production often keep records or notations of personal and financial information of victims or intended victims. These records often include the victim's name, date of birth, social security number, driver's license number, true address, employment history and salary, mother's maiden name, true bank and credit account information. Individuals who commit multiple acts of identity theft and related crimes typically maintain records or notations of personal and financial information for months or even years after the information is obtained in order to facilitate further fraud and theft. This information is often stored in email boxes so that it will be readily accessible from any computer or phone and so it can be sent via email to other co-conspirators.

41. Individuals who in engage in fraudulent document production will often keep photographs and other personal information of co-conspirators in order to further facilitate and hasten fraudulent document production. This information is often stored in email boxes so that it is readily accessible from any computer of phone and can be sent via email to other co-conspirators.

SERVICE AND EXECUTION

42. Under 18 U.S.C. § 2703(g), a law enforcement officer does not have to be present for either the service or execution of the warrant. I request that Oath Holdings, Inc. be required to produce the electronic communications and other information identified in Attachment A hereto. Because Oath Holdings, Inc. is not aware of the facts of this investigation, its employees are not in a position to search for relevant evidence. In addition, requiring Oath Holdings, Inc. to perform the search would be a burden upon the company. If all Oath Holdings, Inc. are asked to

do is produce all the files in the account, an employee can do that easily. Requiring Oath Holdings, Inc. employees to search the materials to determine what content is relevant would add to their burden.

43. I request that the Court authorize law enforcement agents to seize only those items identified in Attachment B from what is produced by Oath Holdings, Inc. pursuant to the search warrant. In reviewing these messages, I will treat them in the same way as if I were searching a file cabinet for certain documents. E-mails will be scanned quickly to determine if they are relevant to my search. If they are, they will be read. If I determine that they are not relevant, I will put them aside without reading them in full. This method is similar to what a law enforcement officer would do in the search of a filing cabinet or a seized computer.

44. Under 18 U.S.C. § 2703(b)(1)(A), notice to the customer or subscriber is not required when the government obtains the contents of electronic communications using a search warrant.

45. Under 18 U.S.C. §§ 2711(3) and 3127, this Court has the authority to issue the warrant directing Oath Holdings, Inc. to comply even though neither Oath Holdings, Inc. is located in this district, because the Court has jurisdiction over the offenses being investigated.

46. I also respectfully request that the warrant direct Oath Holdings, Inc. to produce log records and other non-content information pertaining to the subject email accounts. The government may obtain such records either by filing a motion under 18 U.S.C. § 2703(d), or by means of a search warrant under 18 U.S.C. 2703(c)(1)(A). Because I need a search warrant to obtain the electronic communications anyway, I am proceeding in the request for records by search warrant as well. The facts set forth above to show probable cause also constitute specific and articulable facts, showing that there are reasonable grounds to believe that the records and

other information sought are relevant and material to an ongoing criminal investigation, as required by 18 U.S.C. § 2703(d).

47. As explained herein, information stored in connection with an email account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts list, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, email providers typically log the Internet Protocol (“IP”) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user’s account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner’s state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner’s motive and intent to commit a crime (e.g., communications relating to the crime), or

consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

48. I further respectfully request that this Court issue an order sealing, until further order of this Court, all papers submitted in support of this Application, including the Application, Affidavit, and Search Warrants, and the requisite inventory. Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation and premature disclosure of the contents of this Affidavit and related documents may have a negative impact on this continuing investigation and may jeopardize its effectiveness. I further request, pursuant to 18 U.S.C. § 2705(b), that this Court direct Oath Holdings, Inc. not to notify any other person of this warrant until such time as the Court unseals it.

CONCLUSION

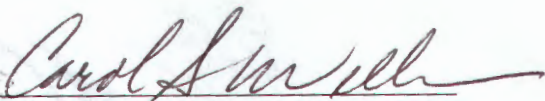
49. Based on the foregoing, I submit that there is probable cause that the items set forth in Attachments B, which constitute evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1028 – identity fraud and 18 U.S.C. § 371 – conspiracy to commit offenses against the United States (i.e., identity fraud) are located in the aforementioned email account, which are hosted on servers owned, maintained, and/or operated by Oath Holdings Inc., headquartered at 701 First Avenue, Sunnyvale, CA 94089.

50. Based upon the above stated information, I respectfully request that this Court issue a warrant to search the email account, and that such search warrant be directed to Oath Holdings Inc. for the purpose of searching the aforementioned email account.



SAMUEL A. BRACKEN
US Postal Inspector
US Postal Inspection Service

Sworn to before me this 13th day of
May 2019:



CAROL SANDRA MOORE WELLS
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A – LOCATION TO BE SEARCHED

(To be served on Oath Holdings Inc.)

This warrant applies to information associated with the Oath Holdings Inc. user IDs and/or email addresses:

- **Stevenhoward76@yahoo.com**

Which is stored at premises owned, maintained, controlled, and/or operated by Oath Holdings Inc., headquartered at 701 First Avenue, Sunnyvale, CA 94089.

ATTACHMENT B

(This page to be served on Oath Holdings Inc.)

I. Information to be disclosed by Oath Holdings Inc. (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A for the time period of June 1, 2016 to the present:

a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and

f. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within 7 days of the issuance of this warrant.

II. Production of Files

Copies of the above-described records and stored information should be obtained from original storage and provided by the following means:

- a. On CD-R (CD-Recordable) or other appropriate digital media, and delivered or mailed to United States Postal Inspector Samuel A. Bracken within 7 days of the issuance of this warrant.

ITEMS TO BE SEIZED BY THE GOVERNMENT – 1 and 2

(This Page Not to be Served on Oath Holdings Inc.)

Agents for the government may search that materials produced by Oath Holdings Inc. for the following items:

All information for the time period of June 1, 2016 to the present as described below that constitutes evidence, fruits or instrumentalities of violations of 18 U.S.C. § 1028(a) – Identity Fraud; and 18 U.S.C. § 371 – Conspiracy to commit offenses against the United States, that is:

- (a) Any and all messages and correspondence regarding the ordering of fraudulent identification cards, including photographs of individuals, receipts of payment, and instructions on information requested to appear on the fraudulent identification cards
- (b) Receipts, letters, emails, and other correspondence from Western Union and/or MoneyGram
- (c) Use of identity information, to include names; dates of birth; Social Security numbers; driver's license or state-issued identification information.
- (d) Evidence indicating how and when the email account was accessed or used.
- (e) Information indicating the identity of the users and/or creators of the subject account.
- (f) Information showing the identity of the person(s) who communicated with the user IDs listed in all Attachment As about matters relating to the identity theft scheme set forth in the Affidavit, including co-conspirators known and unknown to the government, including records that help reveal their whereabouts.
- (g) Information concerning how any identity information was acquired; about the gathering and distribution of any goods, profits, or proceeds from the scheme described

in the affidavit; and evidence of the use of identifying information, to include receipts, transactional statements, and order information.